

## CYCLIC CODES FROM DICKSON POLYNOMIALS

CUNSHENG DING

**ABSTRACT.** Due to their efficient encoding and decoding algorithms cyclic codes, a subclass of linear codes, have applications in consumer electronics, data storage systems, and communication systems. In this paper, Dickson polynomials of the first and second kind over finite fields are employed to construct a number of classes of cyclic codes. Lower bounds on the minimum weight of some classes of the cyclic codes are developed. The minimum weights of some other classes of the codes constructed in this paper are determined. The dimensions of the codes obtained in this paper are flexible. Most of the codes presented in this paper are optimal or almost optimal in the sense that they meet some bound on linear codes. Over ninety cyclic codes of this paper should be used to update the current database of tables of best linear codes known. Among them sixty are optimal in the sense that they meet some bound on linear codes and the rest are cyclic codes having the same parameters as the best linear code in the current database maintained at <http://www.codetables.de/>.

## 1. INTRODUCTION

Let  $q$  be a power of a prime  $p$ . A linear  $[n, k, d]$  code over  $\text{GF}(q)$  is a  $k$ -dimensional subspace of  $\text{GF}(q)^n$  with minimum (Hamming) nonzero weight  $d$ . A linear  $[n, k]$  code  $C$  over the finite field  $\text{GF}(q)$  is called *cyclic* if  $(c_0, c_1, \dots, c_{n-1}) \in C$  implies  $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ . Let  $\gcd(n, q) = 1$ . By identifying any vector  $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$  with

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \text{GF}(q)[x]/(x^n - 1),$$

any code  $C$  of length  $n$  over  $\text{GF}(q)$  corresponds to a subset of  $\text{GF}(q)[x]/(x^n - 1)$ . The linear code  $C$  is cyclic if and only if the corresponding subset in  $\text{GF}(q)[x]/(x^n - 1)$  is an ideal of the ring  $\text{GF}(q)[x]/(x^n - 1)$ . It is well known that every ideal of  $\text{GF}(q)[x]/(x^n - 1)$  is principal. Let  $C = (g(x))$  be a cyclic code. Then  $g(x)$  is called the *generator polynomial* and  $h(x) = (x^n - 1)/g(x)$  is referred to as the *parity-check polynomial* of  $C$ .

A vector  $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$  is said to be *even-like* if  $\sum_{i=0}^{n-1} c_i = 0$ , and is *odd-like* otherwise. The minimum weight of the even-like codewords, respectively the odd-like codewords of a code is the minimum even-like weight, denoted by  $d_{\text{even}}$ , respectively the minimum odd-like weight of the code, denoted by  $d_{\text{odd}}$ . The *even-like subcode* of a linear code consists of all the even-like codewords of this linear code.

The error correcting capability of cyclic codes may not be as good as some other linear codes in general. However, cyclic codes have wide applications in storage and communication systems because they have efficient encoding and decoding algorithms [4, 9, 15]. For example, Reed-Solomon codes have found important applications from deep-space communication to consumer electronics. They are prominently used in consumer electronics such as CDs, DVDs, Blu-ray Discs, in data transmission technologies such as DSL &

---

*Date:* March 8, 2013.

*Key words and phrases.* Dickson polynomials, cyclic codes, linear span, sequences.

WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems.

Cyclic codes have been studied for decades and a lot of progress has been made (see for example, [3, 11, 14]). The total number of cyclic codes over  $\text{GF}(q)$  and their constructions are closely related to cyclotomic cosets modulo  $n$ , and thus many areas of number theory. One way of constructing cyclic codes over  $\text{GF}(q)$  with length  $n$  is to use the generator polynomial

$$(1) \quad \frac{x^n - 1}{\gcd(S(x), x^n - 1)}$$

where

$$S(x) = \sum_{i=0}^{n-1} s_i x^i \in \text{GF}(q)[x]$$

and  $s^\infty = (s_i)_{i=0}^\infty$  is a sequence of period  $n$  over  $\text{GF}(q)$ . Throughout this paper, we call the cyclic code  $C_s$  with the generator polynomial of (1) the *code defined by the sequence  $s^\infty$* , and the sequence  $s^\infty$  the *defining sequence* of the cyclic code  $C_s$ .

One basic question is whether good cyclic codes can be constructed with this approach. It will be demonstrated in this paper that the code  $C_s$  could be an optimal or almost optimal linear code if the sequence  $s^\infty$  is properly designed.

In this paper, Dickson polynomials over finite fields will be employed to construct a number of classes of cyclic codes. Lower bounds on the minimum weight of some classes of the cyclic codes are developed. The minimum weights of some other classes of the codes constructed in this paper are determined. The dimensions of the codes of this paper are flexible. It is amazing that most of the cyclic codes from Dickson polynomials of the first kind with small degrees are optimal or almost optimal in the sense that they meet some bound on the parameters of linear codes. Over ninety cyclic codes of this paper should be used to update the current database of tables of best linear codes known maintained by Markus Grassl at <http://www.codetables.de/>. Among them sixty are optimal in the sense that they meet some bound on linear codes and the rest are cyclic codes having the same parameters as the best linear code in the current database maintained at <http://www.codetables.de/>. The optimality of many of these cyclic codes is the major motivation of this paper. Another motivation of this study is the simplicity of the constructions of the cyclic codes in this paper.

## 2. PRELIMINARIES

In this section, we present basic notations and results of Dickson polynomials,  $q$ -cyclotomic cosets, and sequences that will be employed in subsequent sections.

**2.1. Some notations fixed throughout this paper.** Throughout this paper, we adopt the following notations unless otherwise stated:

- $p$  is a prime.
- $q$  is a positive power of  $p$ .
- $m$  is a positive integer.
- $r = q^m$ .
- $n = q^m - 1$ .
- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  denotes the ring associated with the modulo- $n$  addition and modulo- $n$  multiplication operations.
- $\alpha$  is a generator of  $\text{GF}(r)^*$ .
- $m_a(x)$  is the minimal polynomial of  $a \in \text{GF}(r)$  over  $\text{GF}(q)$ .

- $\text{Tr}(x)$  is the trace function from  $\text{GF}(r)$  to  $\text{GF}(q)$ .
- $\delta(x)$  is a function on  $\text{GF}(r)$  defined by  $\delta(x) = 0$  if  $\text{Tr}(x) = 0$  and  $\delta(x) = 1$  otherwise.
- For any polynomial  $g(x) \in \text{GF}(q)[x]$  with  $g(0) \neq 0$ ,  $\bar{g}(x)$  denotes the reciprocal of  $g(x)$ .
- For any code  $C$  over  $\text{GF}(q)$  with generator polynomial  $g(x)$ ,  $\bar{C}$  denotes the cyclic code with generator polynomial  $\bar{g}(x)$ . It is well known that  $C$  and  $\bar{C}$  have the same weight distribution.
- By the Database we mean the collection of the tables of best linear codes known maintained by Markus Grassl at <http://www.codetables.de/>.

**2.2. The  $q$ -cyclotomic cosets modulo  $n = q^m - 1$ .** The  $q$ -cyclotomic coset containing  $j$  modulo  $n$  is defined by

$$C_j = \{j, qj, q^2j, \dots, q^{\ell_j-1}j\} \subset \mathbb{Z}_n$$

where  $\ell_j$  is the smallest positive integer such that  $q^{\ell_j-1}j \equiv j \pmod{n}$ , and is called the size of  $C_j$ . It is known that  $\ell_j$  divides  $n$ . The smallest integer in  $C_j$  is called the *coset leader* of  $C_j$ . Let  $\Gamma$  denote the set of all coset leaders. By definition, we have

$$\bigcup_{j \in \Gamma} C_j = \mathbb{Z}_n.$$

It is easily seen that  $\ell_i = \ell_{n-i}$  for all  $i$ .

It is well known that each  $\prod_{j \in C_i} (x - \alpha^j)$  is an irreducible polynomial of degree  $\ell_i$  over  $\text{GF}(q)$  and

$$x^n - 1 = \prod_{i \in \Gamma} \prod_{j \in C_i} (x - \alpha^j)$$

where  $\alpha$  is a generator of  $\text{GF}(r)^*$ .

**2.3. The linear span and minimal polynomial of sequences.** Let  $s^L = s_0s_1 \dots s_{L-1}$  be a sequence over  $\text{GF}(q)$ . The *linear span* (also called *linear complexity*) of  $s^L$  is defined to be the smallest positive integer  $\ell$  such that there are constants  $c_0 = 1, c_1, \dots, c_\ell \in \text{GF}(q)$  satisfying

$$-c_0s_i = c_1s_{i-1} + c_2s_{i-2} + \dots + c_\ell s_{i-\ell} \text{ for all } \ell \leq i < L.$$

In engineering terms, such a polynomial  $c(x) = c_0 + c_1x + \dots + c_\ell x^\ell$  is called the *feedback polynomial* of a shortest linear feedback shift register (LFSR) that generates  $s^L$ . Such an integer always exists for finite sequences  $s^L$ . When  $L$  is  $\infty$ , a sequence  $s^\infty$  is called a semi-infinite sequence. If there is no such an integer for a semi-infinite sequence  $s^\infty$ , its linear span is defined to be  $\infty$ . The linear span of the zero sequence is defined to be zero. For ultimately periodic semi-infinite sequences such an  $\ell$  always exists.

Let  $s^\infty$  be a sequence of period  $L$  over  $\text{GF}(q)$ . Any feedback polynomial of  $s^\infty$  is called a *characteristic polynomial*. The characteristic polynomial with the smallest degree is called the *minimal polynomial* of the periodic sequence  $s^\infty$ . Since we require that the constant term of any characteristic polynomial be 1, the minimal polynomial of any periodic sequence  $s^\infty$  must be unique. In addition, any characteristic polynomial must be a multiple of the minimal polynomial.

For periodic sequences, there are a few ways to determine their linear span and minimal polynomials. One of them is given in the following lemma [13].

**Lemma 2.1.** *Let  $s^\infty$  be a sequence of period  $L$  over  $\text{GF}(q)$ . Define*

$$S^L(x) = s_0 + s_1x + \dots + s_{L-1}x^{L-1} \in \text{GF}(q)[x].$$

Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by

$$(2) \quad \frac{x^L - 1}{\gcd(x^L - 1, S^L(x))}$$

and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$(3) \quad L - \deg(\gcd(x^L - 1, S^L(x))).$$

The other one is given in the following lemma [1]

**Lemma 2.2.** Any sequence  $s^\infty$  over  $\text{GF}(q)$  of period  $q^m - 1$  has a unique expansion of the form

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it}, \text{ for all } t \geq 0,$$

where  $\alpha$  is a generator of  $\text{GF}(q^m)^*$  and  $c_i \in \text{GF}(q^m)$ . Let the index set  $I = \{i \mid c_i \neq 0\}$ , then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is

$$\mathbb{M}_s(x) = \prod_{i \in I} (1 - \alpha^i x),$$

and the linear span of  $s^\infty$  is  $|I|$ .

It should be noticed that in some references the reciprocal of  $\mathbb{M}_s(x)$  is called the minimal polynomial of the sequence  $s^\infty$ . So Lemma 2.2 is a modified version of the original one in [1].

**2.4. Dickson polynomials over finite fields  $\text{GF}(r)$ .** One hundred and sixteen years ago Dickson introduced the following family of polynomials over the finite field  $\text{GF}(r)$  [6]:

$$(4) \quad D_h(x, a) = \sum_{i=0}^{\lfloor \frac{h}{2} \rfloor} \frac{h}{h-i} \binom{h-i}{i} (-a)^i x^{h-2i},$$

where  $a \in \text{GF}(r)$  and  $h \geq 0$  is called the *order* of the polynomial. This family is referred to as the *Dickson polynomials of the first kind*.

It is known that Dickson polynomials of the first kind satisfy the following recurrence relation:

$$(5) \quad D_{h+2}(x, a) = x D_{h+1}(x, a) - a D_h(x, a)$$

with the initial state  $D_0(x, a) = 2$  and  $D_1(x, a) = x$ .

Dickson polynomials of the second kind over the finite field  $\text{GF}(r)$  are defined by

$$(6) \quad E_h(x, a) = \sum_{i=0}^{\lfloor \frac{h}{2} \rfloor} \binom{h-i}{i} (-a)^i x^{h-2i},$$

where  $a \in \text{GF}(r)$  and  $h \geq 0$  is called the *order* of the polynomial. This family is referred to as the *Dickson polynomials of the second kind*.

It is known that Dickson polynomials of the second kind satisfy the following recurrence:

$$(7) \quad E_{h+2}(x, a) = x E_{h+1}(x, a) - a E_h(x, a)$$

with the initial state  $E_0(x, a) = 1$  and  $E_1(x, a) = x$ .

Dickson polynomials are an interesting topic of mathematics, and have many applications. For example, the Dickson polynomials  $D_5(x, a) = x^5 - ux - u^2x$  over  $\text{GF}(3^m)$  are employed to construct a family of planar functions [5, 8], and those planar functions give

two families of commutative presemifields, planes, several classes of linear codes [2, 16], and two families of skew Hadamard difference sets [8]. The reader is referred to [12] for detailed information about Dickson polynomials. In this paper, we will employ Dickson polynomials of both kinds over finite fields to construct cyclic codes.

### 3. THE CONSTRUCTION OF CYCLIC CODES FROM POLYNOMIALS OVER $\text{GF}(r)$

Given any polynomial  $f(x)$  on  $\text{GF}(r)$ , we define its associated sequence  $s^\infty$  by

$$(8) \quad s_i = \text{Tr}(f(\alpha^i + 1))$$

for all  $i \geq 0$ , where  $\alpha$  is a generator of  $\text{GF}(r)^*$  and  $\text{Tr}(x)$  denotes the trace function from  $\text{GF}(r)$  to  $\text{GF}(q)$ .

The objective of this section is to consider cyclic codes  $C_s$  defined by Dickson polynomial over  $\text{GF}(r)$  with small degrees.

### 4. CYCLIC CODES FROM THE DICKSON POLYNOMIAL $D_{p^u}(x, a)$

Since  $q$  is a power of  $p$ , it is known that  $D_{hp}(x, a) = D_h(x, a)^p$  [12, Lemma 2.6]. It then follows that

$$D_{p^u}(x, a) = x^{p^u}$$

for all  $a \in \text{GF}(r)$ .

The code  $C_s$  over  $\text{GF}(q)$  defined by the Dickson polynomial  $f(x) = D_{p^u}(x, a) = x^{p^u}$  over  $\text{GF}(q^m)$  may not be new. However, for the completeness of cyclic codes from Dickson polynomials we state the following theorem without giving a proof.

**Theorem 4.1.** *The code  $C_s$  defined by the Dickson polynomial  $D_{p^u}(x, a) = x^{p^u}$  has parameters  $[n, n - m - \delta(1), d]$  and generator polynomial  $\mathbb{M}_s(x) = (x - 1)^{\delta(1)} \mathbb{M}_{\alpha^{-p^u}}(x)$ , where*

$$\begin{cases} d = 4 \text{ if } q = 2 \text{ and } \delta(1) = 1, \\ d = 3 \text{ if } q = 2 \text{ and } \delta(1) = 0, \\ d = 3 \text{ if } q > 2 \text{ and } \delta(1) = 1, \\ d = 2 \text{ if } q > 2 \text{ and } \delta(1) = 0, \end{cases}$$

where the function  $\delta(x)$  and the polynomial  $\mathbb{M}_{\alpha^i}(x)$  were defined in Section 2.1.

When  $q = 2$ , the code of Theorem 4.1 should be equivalent to the binary Hamming weight or its even-weight subcode, and is thus optimal.

Examples of the code of Theorem 4.1 are summarized in Table 1, where the generator  $\alpha$  of  $\text{GF}(r)^*$  is fixed by its minimal polynomial  $m_\alpha^{(q,m)}$  given in Table 9, and the entry "Bd" refers to the upper bound in the Database. The upper bound may or may not be achievable. If a cyclic code or linear code does not meet this upper bound, it does not mean that the code is not optimal. However, if an upper bound is achieved by a code, this code must be optimal, and we put "Yes" in the column "Opt." in the table. If we put "No" in the entry "Opt." in a table, it means that the minum weight of this cyclic code is smaller than of the best linear code with the same length and dimension in the Database. If we put "Maybe" in the entry "Opt.", it means that the cyclic code of this paper has the same parameters as the best linear code in the database that may be optimal.

The Database maintained at <http://www.codetables.de/> is a collection of tables of linear codes over  $\text{GF}(q)$  of length up to 255 that are either optimal or the best known, where  $2 \leq q \leq 9$ . Most of the linear codes in the Database are optimal or almost optimal, but not cyclic. Whenever, an optimal cyclic code or a cyclic code having the same parameters as the best linear code in the Database is discovered, the cyclic code should be used to

replace the noncyclic linear code in the Database as cyclic codes have efficient encoding and decoding algorithms. In this table and other tables in the sequel, the column "DB" indicates if this cyclic code should be used to update the Database.

TABLE 1. Cyclic codes from  $D_{p^h}(x, a)$

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	Thm.	DB
7	3	4	3	2	1	4	Yes	4.1	Yes
15	11	3	4	2	1	3	Yes	4.1	Yes
31	25	4	5	2	1	4	Yes	4.1	Yes
63	57	3	6	2	1	3	Yes	4.1	Yes
127	119	4	7	2	1	4	Yes	4.1	Yes
255	247	3	8	2	1	3	Yes	4.1	Yes
8	5	3	2	3	1	3	Yes	4.1	Yes
26	23	2	3	3	1	2	Yes	4.1	Yes
80	75	3	4	3	1	3	Yes	4.1	Yes
242	236	3	5	3	1	3	Yes	4.1	Yes
15	13	2	2	4	1	2	Yes	4.1	Yes
63	59	3	3	4	1	3	Yes	4.1	Yes
225	251	2	4	4	1	2	Yes	4.1	Yes
24	21	3	2	5	1	3	Yes	4.1	Yes
124	120	3	3	5	1	3	Yes	4.1	Yes
6	5	2	1	7	1	2	Yes	4.1	Yes
48	45	3	2	7	1	3	Yes	4.1	Yes
8	6	3	1	9	1	3	Yes	4.1	Yes
80	77	3	2	9	1	2	Yes	4.1	Yes

## 5. CYCLIC CODES FROM $D_2(x, a) = x^2 - 2a$

In this section we consider the code  $C_s$  defined by  $f(x) = D_2(x, a) = x^2 - 2a$  over  $\text{GF}(r)$ . When  $p = 2$ , this code was treated in Section 4. When  $p > 2$ , the following theorem is a variant of Theorem 3.2 in [7], and is documented here to show the importance of the Dickson polynomials in coding theory.

**Theorem 5.1.** *Let  $p > 2$ . The code  $C_s$  defined by  $f(x) = D_2(x, a) = x^2 - 2a$  has parameters  $[n, n - 2m - \delta(1 - 2a), d]$  and generator polynomial*

$$\mathbb{M}_s(x) = (x - 1)^{\delta(1-2a)} m_{\alpha^{-1}}(x) m_{\alpha^{-2}}(x),$$

where

$$\begin{cases} d = 4 & \text{if } q = 3 \text{ and } \delta(1 - 2a) = 0, \\ 4 \leq d \leq 5 & \text{if } q = 3 \text{ and } \delta(1 - 2a) = 1, \\ d = 3 & \text{if } q > 3 \text{ and } \delta(1 - 2a) = 0, \\ 3 \leq d \leq 4 & \text{if } q > 3 \text{ and } \delta(1 - 2a) = 1, \end{cases}$$

and the function  $\delta(x)$  and the polynomial  $\mathbb{M}_{\alpha^j}(x)$  were defined in Section 2.1.

Examples of the code of Theorem 5.1 are summarized in Table 8, where the meanings of the entries are the same as those in Table 1.

TABLE 2. Cyclic codes from  $D_2(x, a)$ 

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	Thm.	DB
8	3	5	2	3	0	5	Yes	5.1	Yes
8	4	4	2	3	-1	4	Yes	5.1	Yes
26	20	4	3	3	0	4	Yes	5.1	Yes
26	19	5	3	3	$\alpha^2$	5	Yes	5.1	Yes
80	71	5	4	3	0	5	Yes	5.1	Yes
24	19	4	2	5	0	4	Yes	5.1	Yes
24	20	3	2	5	-2	4	AOP	5.1	No
124	117	4	3	5	0	4	Yes	5.1	Yes
124	118	3	3	5	-2	4	AOP	5.1	No
48	43	4	2	7	0	4	Yes	5.1	Yes
48	44	3	2	7	$\alpha$	4	AOP	5.1	Yes
8	6	3	1	9	1	3	Yes	5.1	Yes
80	77	3	2	9	$\alpha$	3	AOP	5.1	Yes

6. CYCLIC CODES FROM  $D_3(x, a) = x^3 - 3ax$ 

In this section we study the code  $C_s$  defined by the Dickson polynomial  $D_3(x, a) = x^3 - 3ax$ . We need to distinguish among the three cases:  $p = 2$ ,  $p = 3$  and  $p \geq 5$ . The case that  $p = 3$  was covered in Section 4. So we need to consider only the two remaining cases.

We first handle the case  $q = p = 2$  and prove the following lemma.

**Lemma 6.1.** *Let  $q = p = 2$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_3(x, a) = x^3 - 3ax = x^3 + ax$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-3}}(x) & \text{if } a = 0, \\ (x-1)^{\delta(1+a)} m_{\alpha^{-1}}(x) m_{\alpha^{-3}}(x) & \text{if } a \neq 0 \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + m & \text{if } a = 0, \\ \delta(1+a) + 2m & \text{if } a \neq 0. \end{cases}$$

*Proof.* Note that

$$D_3(x+1, a) = x^3 + x^2 + (1+a)x + 1 + a.$$

We have then

$$\text{Tr}(D_3(x+1, a)) = \text{Tr}(x^3 + ax) + \text{Tr}(1 + a).$$

By definition,

$$(9) \quad s_t = \text{Tr}((\alpha^t)^3 + a\alpha^t) + \text{Tr}(1 + a).$$

It can be easily proved that  $\ell_1 = \ell_{n-1} = \ell_3 = \ell_{n-3} = m$  and that  $C_1 \cap C_3 = \emptyset$ . The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (9).  $\square$

The following theorem gives information on the code  $C_s$ .

**Theorem 6.2.** *Let  $q = p = 2$ . Then the binary code  $C_s$  defined by the sequence of Lemma 6.1 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 6.1, and*

$$\begin{cases} d = 2 & \text{if } a = 0 \text{ and } \delta(1) = 0, \\ d = 4 & \text{if } a = 0 \text{ and } \delta(1) = 1, \\ d \geq 5 & \text{if } a \neq 0 \text{ and } \delta(1+a) = 0, \\ d \geq 6 & \text{if } a \neq 0 \text{ and } \delta(1+a) = 1. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 6.1 and the definition of the code  $C_s$ . We need to prove the conclusion on the minimum distance  $d$  of  $C_s$ .

We consider the case  $a = 0$  first. Since  $\alpha^3 \neq 0$ ,  $d \geq 2$ . On the other hand, if  $\delta(1) = 0$ , then  $m$  is even and  $(\alpha^3)^{(2^m-1)/3} = 1$ . Hence  $C_s$  has a codeword of Hamming weight 2. Whence,  $d = 2$ . If  $\delta(1) = 1$ , then  $m$  is odd and  $\gcd(3, 2^m - 1) = 1$ . Hence,  $\alpha^3$  is a primitive element of  $\text{GF}(2^m)$  and the code  $\tilde{C}_s$  generated by  $\mathbb{M}_{\alpha^{-3}}(x)$  has minimum weight 3. Hence the even-weight subcode  $C_s$  of  $\tilde{C}_s$  has minimum weight 4.

We now consider the case that  $a \neq 0$ . Note that the reciprocal  $\tilde{\mathbb{M}}_s(x)$  of  $\mathbb{M}_s(x)$  has zeros  $\alpha^i$  for all  $i \in \{1, 2, 3, 4\}$ , and the additional zero  $\alpha^0$  when  $\delta(1+a) = 1$ . The conclusions on the minimum weight  $d$  in this case follow from the BCH bound.  $\square$

**Remark 6.3.** *When  $a = 0$  and  $\delta(1) = 1$ , the code may be equivalent to the even-weight subcode of the Hamming code. We are mainly interested in the case that  $a \neq 0$ . When  $a = 1$ , the code  $C_s$  should be equivalent to the double-error correcting binary BCH code or its even-weight subcode. Theorem 6.2 shows that well-known classes of cyclic codes can be constructed with Dickson polynomials of order 3.*

Examples of the code of Theorem 6.2 are summarized in Table 3, where the meanings of the entries are the same as those in Table 1.

Now we consider the case  $q = p^t$ , where  $p \geq 5$  or  $p = 2$  and  $t \geq 2$ .

**Lemma 6.4.** *Let  $q = p^t$ , where  $p \geq 5$  or  $p = 2$  and  $t \geq 2$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_3(x, a) = x^3 - 3ax$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(-2)} m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) & \text{if } a = 1, \\ (x-1)^{\delta(1-3a)} m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-1}}(x) & \text{if } a \neq 1 \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(-2) + 2m & \text{if } a = 1, \\ \delta(1+a) + 3m & \text{if } a \neq 1. \end{cases}$$

*Proof.* Note that

$$D_3(x+1, a) = x^3 + 3x^2 + 3(1-a)x + 1 - 3a.$$

We have then

$$(10) \quad s_t = \text{Tr}((\alpha^t)^3 + 3(\alpha^t)^2 + 3(1-a)\alpha^t) + \text{Tr}(1-3a).$$

Since  $q = p^t$ , where  $p \geq 5$  or  $p = 2$  and  $t \geq 2$ , one can prove that  $\ell_1 = \ell_{n-1} = \ell_3 = \ell_{n-3} = \ell_2 = \ell_{n-2} = m$  and that

$$C_1 \cap C_2 = \emptyset, C_1 \cap C_3 = \emptyset, C_2 \cap C_3 = \emptyset.$$

The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (10).  $\square$

The following theorem provides information on the code  $C_s$ .



**Theorem 6.5.** *Let  $q = p^t$ , where  $p \geq 5$  or  $p = 2$  and  $t \geq 2$ . Then the code  $C_s$  defined by the sequence of Lemma 6.4 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 6.4, and*

$$\begin{cases} d \geq 3 & \text{if } a = 1, \\ d \geq 4 & \text{if } a \neq 1 \text{ and } \delta(1 - 3a) = 0, \\ d \geq 5 & \text{if } a \neq 1 \text{ and } \delta(1 - 3a) = 1, \\ d \geq 5 & \text{if } a \neq 1 \text{ and } \delta(1 - 3a) = 0 \text{ and } q = 4, \\ d \geq 6 & \text{if } a \neq 1 \text{ and } \delta(1 - 3a) = 1 \text{ and } q = 4. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 6.4 and the definition of the code  $C_s$ . We need to prove the conclusion on the minimum distance  $d$  of  $C_s$ .

Note that  $\bar{\mathbb{M}}_s(x)$  has the zeros  $\alpha^2$  and  $\alpha^3$ . By the BCH bound,  $d \geq 3$  for all cases. If  $a \neq 1$ ,  $\bar{\mathbb{M}}_s(x)$  has the zeros  $\alpha^i$  for all  $i \in \{1, 2, 3\}$  and the additional zero  $\alpha^0$  if  $\delta(1 - 3a) = 1$ . Hence, the second and third lower bound on  $d$  follow also from the BCH bound.

The case  $q = 4$  is special. In this case,  $\bar{\mathbb{M}}_s(x)$  has the zeros  $\alpha^i$  for all  $i \in \{1, 2, 3, 4\}$  and the additional zero  $\alpha^0$  if  $\delta(1 - 3a) = 1$ . Hence, the last two lower bounds on  $d$  also follow from the BCH bound.  $\square$

Examples of the code of Theorem 6.5 are summarized in Table 3, where the meanings of the entries are the same as those in Table 1.

TABLE 3. Cyclic codes from  $D_3(x, a)$

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	Thm.	DB
15	6	6	4	2	$\alpha^3$	6	Yes	6.2	Yes
15	7	5	4	2	1	5	Yes	6.2	Yes
31	20	6	5	2	$\alpha^4$	6	Yes	6.2	Yes
31	21	5	5	2	$\alpha^3$	5	Yes	6.2	Yes
63	50	6	6	2	$\alpha^3$	6	Yes	6.2	Yes
63	51	5	6	2	$\alpha^4$	5	Yes	6.2	Yes
127	112	6	7	2	$\alpha^5$	6	Yes	6.2	Yes
127	113	5	7	2	$\alpha^7$	5	Yes	6.2	Yes
15	8	6	2	4	$\alpha$	6	Yes	6.5	Yes
15	9	5	2	4	0	5	Yes	6.5	Yes
63	53	6	3	4	$\alpha^2$	6	Yes	6.5	Yes
63	54	5	3	4	$\alpha$	5	Yes	6.5	Yes
255	242	6	4	4	$\alpha^2$	6	Yes	6.5	Yes
255	243	5	4	4	0	6	Maybe	6.5	Yes
24	17	5	2	5	$\alpha^3$	5	AOP	6.5	No
24	18	4	2	5	$\alpha^6$	5	AOP	6.5	No
24	19	4	2	5	1	4	Yes	6.5	Yes
124	114	5	3	5	$\alpha$	6	Maybe	6.5	Yes
124	117	4	3	5	1	4	Yes	6.5	Yes
48	41	5	2	7	0	6	Maybe	6.5	Yes
48	42	4	2	7	$\alpha^2$	5	Maybe	6.5	Yes
48	43	3	2	7	1	4	AOP	6.5	No

### 7. CYCLIC CODES FROM $D_4(x, a) = x^4 - 4ax^2 + 2a^2$

In this section we investigate the code  $C_s$  defined by the Dickson polynomial  $D_4(x, a) = x^4 - 4ax^2 + 2a^2$ . We have to distinguish among the three cases:  $p = 2$ ,  $p = 3$  and  $p \geq 5$ . The case that  $p = 2$  was covered in Section 4. So we need to consider only the two remaining cases.

We first take care of the case  $q = p = 3$  and prove the following lemma.

**Lemma 7.1.** *Let  $q = p = 3$  and  $m \geq 3$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_4(x, a) = x^4 - 4ax^2 + 2a^2$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-1}}(x) & \text{if } a = 0, \\ (x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x) & \text{if } a = 1, \\ (x-1)^{\delta(1-a-a^2)} m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-1}}(x) & \text{otherwise} \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + 2m & \text{if } a = 0, \\ \delta(1) + 2m & \text{if } a = 1, \\ \delta(1-a-a^2) + 3m & \text{otherwise.} \end{cases}$$

*Proof.* Note that

$$D_4(x+1, a) = x^4 + x^3 - ax^2 + (1+a)x + 1 - a - a^2.$$

We have then

$$\text{Tr}(D_4(x+1, a)) = \text{Tr}(x^4 - ax^2 + (a-1)x) + \text{Tr}(1 - a - a^2).$$

By definition,

$$(11) \quad s_t = \text{Tr}((\alpha^t)^4 - a(\alpha^t)^2 + (a-1)\alpha^t) + \text{Tr}(1 - a - a^2).$$

It can be easily proved that  $\ell_1 = \ell_{n-1} = \ell_4 = \ell_{n-4} = \ell_2 = \ell_{n-2} = m$  and that the 3-cyclotomic cosets  $C_1$ ,  $C_2$  and  $C_4$  pairwise disjoint. The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (11).  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 7.2.** *Let  $q = p = 3$  and  $m \geq 3$ . Then the code  $C_s$  defined by the sequence of Lemma 7.1 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 7.1, and*

$$\begin{cases} d = 2 & \text{if } a = 1, \\ d = 3 & \text{if } a = 0 \text{ and } m \equiv 0 \pmod{6}, \\ d \geq 4 & \text{if } a = 0 \text{ and } m \not\equiv 0 \pmod{6}, \\ d \geq 5 & \text{if } a \neq 0 \text{ and } \delta(1-a-a^2) = 0, \\ d \geq 6 & \text{if } a \neq 0 \text{ and } \delta(1-a-a^2) \neq 0. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 7.1 and the definition of the code  $C_s$ . We need to prove only the conclusion on the minimum distance  $d$  of  $C_s$ .

We consider the case  $a = 1$  first. In this case, the generator polynomial of this code  $C_s$  is  $(x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x)$ . It is easily seen that  $1$ ,  $\alpha^{-2}$  and  $\alpha^{-4}$  are roots of  $2 + x^{(3^m-1)/2} = 0$ . Therefore,  $C_s$  has the codeword  $2 + x^{(3^m-1)/2}$  of Hamming weight 2. Hence  $d = 2$  when  $a = 1$ .

We now treat the case  $a = 0$ . In this case, the generator polynomial of this code is  $\mathbb{M}_s(x) = (x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-1}}(x)$ . Note that  $\bar{\mathbb{M}}_s(x)$  has the zeros  $\alpha^3$  and  $\alpha^4$ . By the BCH bound the minimum weight  $d$  in  $\mathcal{C}_s$  is at least 3. We want to know when  $\mathcal{C}_s$  and  $\bar{\mathcal{C}}_s$  have a codeword of weight 3.

The code  $\bar{\mathcal{C}}_s$  has a codeword of weight three if and only if there are two integers  $t_1$  and  $t_2$  with  $1 \leq t_1 \neq t_2 \leq n-1$  and two elements  $u_1$  and  $u_2$  in  $\{1, -1\}$  such that

$$(12) \quad \begin{cases} 1 + u_1 \alpha^{t_1} + u_2 \alpha^{t_2} = 0, \\ 1 + u_1 \alpha^{4t_1} + u_2 \alpha^{4t_2} = 0. \end{cases}$$

Suppose now that  $\bar{\mathcal{C}}_s$  has a codeword  $1 + u_1 x^{t_1} + u_2 x^{t_2}$  of weight 3. Combining the two equations of (12) yields

$$(13) \quad (u_1 u_2 + 1) \alpha^{4t_2} + u_2 \alpha^{3t_2} + u_2 \alpha^{t_2} + 1 + u_1 = 0$$

and

$$(14) \quad (u_1 u_2 + 1) \alpha^{4t_1} + u_1 \alpha^{3t_1} + u_1 \alpha^{t_1} + 1 + u_2 = 0.$$

We now consider the first subcase that  $u_1 u_2 = -1$  under the case that  $a = 0$ . In this subcase,  $\delta(1) = m \bmod 3 = 0$  as  $1 + u_1 + u_2 = 1 \neq 0$ . In this subcase (13) and (14) become

$$(15) \quad \alpha^{3t_2} + \alpha^{t_2} - u_1(1 + u_1) = 0$$

and

$$(16) \quad \alpha^{3t_1} + \alpha^{t_1} - u_2(1 + u_2) = 0.$$

Due to symmetry, we assume that  $(u_1, u_2) = (-1, 1)$ . It follows from (15) and (16) that

$$\alpha^{2t_2} = -1 \text{ and } (\alpha^{t_1} - 1)^2 = -1.$$

When  $m$  is odd,  $\alpha^{(3^m-1)/2} = -1$  and  $(3^m-1)/2$  is odd. Hence,  $-1$  cannot be a square in  $\text{GF}(r)$ . Therefore,  $\bar{\mathcal{C}}_s$  cannot have a codeword  $1 + u_1 x^{t_1} + u_2 x^{t_2}$  when  $a = 0$  and  $m$  is odd, where  $u_1 u_2 = -1$ . When  $m$  is even,  $m \equiv 0 \pmod{6}$  and  $-1$  is a square in  $\text{GF}(r)$ . Let  $y_1 \in \text{GF}(r)$  be a solution of  $y^2 = -1$ , and define  $t_2$  and  $t_1$  such that

$$\alpha^{t_2} = y_1, \quad \alpha^{t_1} = 1 + y_1.$$

Then  $t_1$  and  $t_2$  are distinct and  $1 + x^{t_1} - x^{t_2}$  is indeed a codeword of weight three in  $\bar{\mathcal{C}}_s$ . Thus,  $d = 3$  when  $m \equiv 0 \pmod{6}$ .

We are ready to consider the second subcase that  $u_1 u_2 = 1$  under the case that  $a = 0$ . In this subcase (13) and (14) become

$$(17) \quad \alpha^{4t_2} - u_2 \alpha^{3t_2} - u_2 \alpha^{t_2} - (1 + u_1) = 0$$

and

$$(18) \quad \alpha^{4t_1} - u_1 \alpha^{3t_1} - u_1 \alpha^{t_1} - (1 + u_2) = 0$$

When  $(u_1, u_2) = (1, 1)$ . It follows from (17) and (18) that

$$(\alpha^{t_2} - 1)^4 = 0 \text{ and } (\alpha^{t_1} - 1)^4 = 0.$$

Hence  $\alpha^{t_2} = \alpha^{t_1} = 1$ . This is impossible as  $\alpha$  is a generator of  $\text{GF}(r)$ . Therefore,  $\bar{\mathcal{C}}_s$  cannot have a codeword  $1 + x^{t_1} + x^{t_2}$ . When  $(u_1, u_2) = (-1, -1)$ . It follows from (17) and (18) that

$$\begin{aligned} \alpha^{t_2} (\alpha^{3t_2} + \alpha^{2t_2} + 1) &= 0, \\ \alpha^{t_1} (\alpha^{3t_1} + \alpha^{2t_1} + 1) &= 0. \end{aligned}$$

Note that  $y^3 + y^2 + 1 = 0$  if and only if

$$(y^{-1} - 1)^3 + (y^{-1} - 1) = 0.$$

However,  $z^3 + z = 0$  does not have a nonzero solution  $z$  in  $\text{GF}(r)$  if  $m$  is odd. This proves that the code  $\tilde{C}_s$  cannot have a codeword  $1 - x^{t_1} - x^{t_2}$  when  $m$  is odd. If  $m$  is even,  $m \equiv 0 \pmod{6}$  as  $1 + u_1 + u_2 = 1 \neq 0$ . When  $m \equiv 0 \pmod{6}$ , let  $z_1 \in \text{GF}(r)$  and  $z_2 \in \text{GF}(r)$  be the two distinct solutions of  $z^2 = -1$ . Define  $t_1$  and  $t_2$  so that

$$\alpha^{t_i} = \frac{1}{1 + z_i}$$

for  $i \in \{1, 2\}$ . Then  $1 - x^{t_1} - x^{t_2}$  is a codeword of weight three in  $\tilde{C}_s$ . This completes the proof of the conclusions on the minimum weight  $d$  for the case  $a = 0$ .

When  $a(a - 1) \neq 0$ ,  $\mathbb{M}_s(x)$  has the zeros  $\alpha^i$  for all  $i \in \{1, 2, 3, 4\}$  and the additional zero  $\alpha^0$  if  $\delta(1 - a - a^2) = 1$ . The last two lower bounds on  $d$  then follow from the BCH bound.  $\square$

**Remark 7.3.** When  $a = 1$ , the code of Theorem 7.2 is not optimal nor almost optimal. The code in the case that  $a = 0$  has the same length and dimension, but a larger minimum weight.

Examples of the code of Theorem 7.2 are summarized in Table 4, where the meanings of the entries are the same as those in Table 1.

TABLE 4. Cyclic codes from  $D_4(x, a)$

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	Thm.	DB
8	4	4	2	3	0	4	Yes	7.2	Yes
8	2	6	2	3	$\alpha$	6	Yes	7.2	Yes
26	16	6	3	3	$\alpha^3$	7	Maybe	7.2	Yes
26	17	5	3	3	$\alpha^4$	6	AOP	7.2	No
26	20	2	3	3	1	4	No	7.2	No
26	20	4	3	3	0	4	Yes	7.2	Yes
48	39	6	2	7	$\alpha$	8	Maybe	7.5	Yes
48	40	5	2	7	3	7	No	7.5	No
80	67	6	3	3	$\alpha$	7	Maybe	7.2	Yes
80	68	5	3	3	$\alpha^7$	6	AOP	7.2	No
80	71	2	4	3	1	5	No	7.2	No
80	71	4	4	3	0	5	AOP	7.2	No
80	71	6	2	9	$\alpha$	8	Maybe	7.5	Yes
80	72	5	2	9	$\alpha^{16}$	7	Maybe	7.5	Yes
80	73	4	2	9	0	5	AOP	7.5	No
124	111	7	3	5	1	8	Maybe	7.5	Yes
124	112	6	3	5	$\alpha^3$	8	Maybe	7.5	Yes
124	114	4	3	5	4	6	No	7.5	No

Now we consider the case  $q = p^t$ , where  $p \geq 5$  or  $p = 3$  and  $t \geq 2$ .

**Lemma 7.4.** Let  $m \geq 2$  and  $q = p^t$ , where  $p \geq 5$  or  $p = 3$  and  $t \geq 2$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_4(x, a) = x^4 - 4ax^2 + 2a^2$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of

$s^\infty$  is given by

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-1}}(x) & \text{if } a = \frac{3}{2}, \\ (x-1)^{\delta(1)} m_{\alpha^{-4}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) & \text{if } a = \frac{1}{2}, \\ (x-1)^{\delta(1-4a+2a^2)} \prod_{i=1}^4 m_{\alpha^{-i}}(x) & \text{if } a \notin \{\frac{3}{2}, \frac{1}{2}\}. \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + 3m & \text{if } a \in \{\frac{3}{2}, \frac{1}{2}\}, \\ \delta(1 - 4a + 2a^2) + 4m & \text{otherwise.} \end{cases}$$

*Proof.* Note that

$$D_4(x+1, a) = x^4 + 4x^3 + (6-4a)x^2 + (4-8a)x + 1 - 4a + 2a^2.$$

We have then

$$(19) \quad \begin{aligned} s_t &= \text{Tr}((\alpha')^4 + 4(\alpha')^3 + (6-4a)(\alpha')^2 + (4-8a)\alpha') + \\ &\quad \text{Tr}(1 - 4a + 2a^2) \end{aligned}$$

for all  $t \geq 0$ .

Since  $m \geq 2$  and  $q = p^t$ , where  $p \geq 5$  or  $p = 3$  and  $t \geq 2$ , one can prove that

$$\ell_1 = \ell_{n-1} = \ell_3 = \ell_{n-3} = \ell_2 = \ell_{n-2} = \ell_4 = \ell_{n-4} = m$$

and that the  $q$ -cyclotomic cosets  $C_1, C_2, C_3, C_4$  are pairwise disjoint. The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (19).  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 7.5.** *Let  $m \geq 2$  and  $q = p^t$ , where  $p \geq 5$  or  $p = 3$  and  $t \geq 2$ . Then the code  $C_s$  defined by the sequence of Lemma 7.4 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 7.4, and*

$$\begin{cases} d \geq 3 & \text{if } a = \frac{3}{2}, \\ d \geq 4 & \text{if } a = \frac{1}{2}, \\ d \geq 5 & \text{if } a \notin \{\frac{3}{2}, \frac{1}{2}\} \text{ and } \delta(1 - 4a + a^2) = 0, \\ d \geq 6 & \text{if } a \notin \{\frac{3}{2}, \frac{1}{2}\} \text{ and } \delta(1 - 4a + a^2) = 1. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 7.4 and the definition of the code  $C_s$ . The lower bounds on the minimum weight  $d$  of  $C_s$  follow from the BCH bounds. The details are left to the reader.  $\square$

Examples of the code of Theorem 7.5 are summarized in Table 4, where the meanings of the entries are the same as those in Table 1.

## 8. CYCLIC CODES FROM $D_5(x, a) = x^5 - 5ax^3 + 5a^2x$

In this section we deal with the code  $C_s$  defined by the Dickson polynomial  $D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . We have to distinguish among the three cases:  $p = 2$ ,  $p = 3$  and  $p \geq 7$ . The case  $p = 5$  was covered in Section 4. So we need to consider only the remaining cases.

We first prove the following lemma.

**Lemma 8.1.** *The equation  $x + x^2 + x^4 = 0$  has a nonzero solution  $x \in \text{GF}(2^m)$  if and only if  $m \equiv 0 \pmod{3}$ .*

*Proof.* Suppose that  $x + x^2 + x^4 = 0$  for some  $x \in \text{GF}(2^m)^*$ . Then  $(x + x^2 + x^4)^2 = x^2 + x^4 + x^8 = 0$ . Combining the two equations yields  $x + x^8 = 0$ . Hence  $x^7 = 1$ . Since  $x \neq 1$ , this means that  $\gcd(7, 2^m) = 2^{\gcd(3, m)} - 1 = 7$ . Hence  $m \equiv 0 \pmod{3}$ .

Suppose now that  $m \equiv 0 \pmod{3}$ . Let  $m' = m/3$ . Define

$$\pi(y) = \sum_{i=0}^{m'} y^{2^{3i}}$$

for any  $y \in \text{GF}(2^m)$ . It is well known that  $\text{Tr}(y) = 0$  has  $2^{m-1}$  solutions  $y \in \text{GF}(2^m)$ . One of them must satisfy that  $\pi(y) \neq 0$  as the two functions  $\pi(x)$  and  $\text{Tr}(x)$  are clearly different. Let  $y \in \text{GF}(2^m)$  such that  $\text{Tr}(y) = 0$  and  $\pi(y) \neq 0$ . Then it is easily seen that  $\pi(y) + \pi(y)^2 + \pi(y)^4 = \text{Tr}(y) = 0$ . This completes the proof.  $\square$

We first consider the case  $q = p = 2$  and prove the following lemma.

**Lemma 8.2.** *Let  $q = p = 2$  and  $m \geq 5$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) & \text{if } a = 0, \\ (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) m_{\alpha^{-3}}(x) & \text{if } 1 + a + a^3 = 0, \\ (x-1)^{\delta(1)} \prod_{i=0}^2 m_{\alpha^{-(2i+1)}}(x) & \text{if } a + a^2 + a^4 \neq 0 \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + m & \text{if } a = 0, \\ \delta(1) + 2m & \text{if } 1 + a + a^3 = 0, \\ \delta(1) + 3m & \text{if } a + a^2 + a^4 \neq 0. \end{cases}$$

*Proof.* Note that

$$D_5(x+1, a) = x^5 + x^4 + ax^3 + ax^2 + (1+a+a^2)x + 1 + a + a^2.$$

Since  $q = 2$ , we have then

$$\text{Tr}(D_5(x+1, a)) = \text{Tr}\left(x^5 + ax^3 + (a^{2^{m-1}} + a + a^2)x\right) + \text{Tr}(1).$$

By definition,

$$(20) \quad s_t = \text{Tr}\left((\alpha^t)^5 + a(\alpha^t)^3 + (a^{2^{m-1}} + a + a^2)(\alpha^t)\right) + \text{Tr}(1).$$

It can be easily proved that  $\ell_1 = \ell_3 = \ell_5 = m$  and that  $C_1, C_3$  and  $C_5$  are pairwise disjoint when  $m \geq 5$ . The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (20).  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 8.3.** *Let  $q = p = 2$  and  $m \geq 5$ . Then the code  $C_s$  defined by the sequence of Lemma 8.2 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 8.2, and*

$$\begin{cases} d = 2 & \text{if } a = 0 \text{ and } \delta(1) = 0 \text{ and } \gcd(5, n) = 5, \\ d = 3 & \text{if } a = 0 \text{ and } \delta(1) = 0 \text{ and } \gcd(5, n) = 1, \\ d = 4 & \text{if } a = 0 \text{ and } \delta(1) = 1, \\ d \geq 3 & \text{if } 1 + a + a^3 = 0 \text{ and } \delta(1) = 0, \\ d \geq 4 & \text{if } 1 + a + a^3 = 0 \text{ and } \delta(1) = 1, \\ d \geq 7 & \text{if } a + a^2 + a^4 \neq 0 \text{ and } \delta(1) = 0, \\ d \geq 8 & \text{if } a + a^2 + a^4 \neq 0 \text{ and } \delta(1) = 1. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 8.2 and the definition of the code  $C_s$ . We need to prove the conclusion on the minimum distance  $d$  of  $C_s$ .

We consider the case  $a = 0$  first. Since  $\alpha^5 \neq 0$ ,  $d \geq 2$ . On the other hand, if  $\delta(1) = 0$  and  $\gcd(5, n) = 5$ , then  $m$  is even and  $(\alpha^5)^{(2^m-1)/5} = 1$ . Hence  $C_s$  has the codeword  $1 + x^{(2^m-1)/5}$  of Hamming weight 2. Whence,  $d = 2$ . If  $\delta(1) = 0$  and  $\gcd(5, n) = 1$ , then  $\alpha^5$  is a primitive element, the code  $C_s$  is equivalent to the Hamming code. Hence  $d = 3$ . If  $\delta(1) = 1$ , then  $m$  is odd and  $\gcd(5, 2^m - 1) = 1$ . Hence,  $\alpha^5$  is a primitive element of  $\text{GF}(2^m)$  and the code  $\tilde{C}_s$  generated by  $\mathbb{M}_{\alpha^{-5}}(x)$  has minimum weight 3. Hence the even-weight subcode  $C_s$  of  $\tilde{C}_s$  has minimum weight 4.

We now consider the case that  $1 + a + a^3 = 0$ . By Lemma 8.1,  $m \equiv 0 \pmod{3}$ . In this case  $\mathbb{M}_s(x) = (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) m_{\alpha^{-3}}(x)$ . Since  $\mathbb{M}_s(x)$  has the zeros  $\alpha^5$  and  $\alpha^6$ ,  $d \geq 3$ . If  $\delta(1) = 1$ ,  $C_s$  is an even-weight code. Hence  $d \geq 4$ .

We finally consider the case that  $1 + a + a^3 \neq 0$ . Note that  $\mathbb{M}_s(x)$  has zeros  $\alpha^i$  for all  $i \in \{1, 2, 3, 4, 5, 6\}$ , and the additional zero  $\alpha^0$  when  $\delta(1) = 1$ . The conclusions on the minimum weight  $d$  in this case follow from the BCH bound.  $\square$

Examples of the code of Theorem 8.3 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

We now consider the case  $(p, q) = (2, 4)$  and prove the following lemma.

**Lemma 8.4.** *Let  $(p, q) = (2, 4)$  and  $m \geq 3$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) & \text{if } a = 0, \\ (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) & \text{if } a = 1, \\ (x-1)^{\delta(1+a+a^2)} m_{\alpha^{-5}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-1}}(x) & \text{if } a + a^2 \neq 0 \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + m & \text{if } a = 0, \\ \delta(1) + 3m & \text{if } a = 1, \\ \delta(1) + 4m & \text{if } a + a^2 \neq 0. \end{cases}$$

*Proof.* Note that

$$D_5(x+1, a) = x^5 + x^4 + ax^3 + ax^2 + (1+a+a^2)x + 1+a+a^2.$$

Since  $q = 2^2$ , we have then

$$\begin{aligned} \text{Tr}(D_5(x+1, a)) &= \text{Tr}(x^5 + ax^3 + ax^2 + (a+a^2)x) + \\ &\quad \text{Tr}(1+a+a^2). \end{aligned}$$

By definition,

$$\begin{aligned} s_t &= \text{Tr}((\alpha^t)^5 + a(\alpha^t)^3 + a(\alpha^t)^2 + (a+a^2)(\alpha^t)) + \\ (21) \quad &\quad \text{Tr}(1+a+a^2). \end{aligned}$$

It can be easily proved that  $\ell_1 = \ell_2 = \ell_3 = \ell_5 = m$  and that  $C_1, C_2, C_3$  and  $C_5$  are pairwise disjoint when  $m \geq 3$ . The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (21).  $\square$

The following theorem provides information on the code  $C_s$ .

TABLE 5. Cyclic codes from  $D_5(x, a)$ 

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	Thm.	DB
7	3	4	3	2	0	4	Yes	8.3	Yes
15	7	5	4	2	1	5	Yes	8.3	Yes
31	15	8	5	2	1	8	Yes	8.3	Yes
31	25	4	5	2	0	4	Yes	8.3	Yes
63	45	7	6	2	1	8	AOP	8.3	No
63	51	3	6	2	$\alpha^9$	5	No	8.3	No
63	57	3	6	2	0	3	Yes	8.3	Yes
127	105	8	7	2	1	8	Yes	8.3	Yes
127	119	4	7	2	0	4	Yes	8.3	Yes
225	231	7	8	2	$\alpha$	8	AOP	8.3	No
225	247	2	8	2	0	3	AOP	8.3	No
15	8	6	2	4	$\alpha^3$	6	Yes	8.5	Yes
15	9	5	2	4	$\alpha$	5	Yes	8.5	Yes
15	11	3	2	4	1	4	AOP	8.5	No
63	50	7	3	4	$\alpha$	9	Maybe	8.5	Yes
63	53	3	3	4	1	6	No	8.5	No
63	59	3	3	4	0	3	Yes	8.5	Yes
63	52	7	2	8	$\alpha$	8	Maybe	8.7	Yes
63	53	6	2	8	1	7	AOP	8.7	No
63	57	3	2	8	0	4	AOP	8.7	No
8	2	6	2	3	1	6	Yes	8.9	Yes
26	17	4	3	3	1	6	No	8.9	No
26	13	8	3	3	$\alpha$	9	Maybe	8.9	Yes
26	14	7	3	3	$\alpha^2$	8	Maybe	8.9	Yes
80	67	4	4	3	1	7	No	8.9	No
80	63	8	4	3	$\alpha$	10	Maybe	8.9	Yes
80	64	7	4	3	$\alpha^2$	9	No	8.9	No
80	71	4	2	9	$-1$	6	No	8.11	No
80	71	5	2	9	$\alpha^{20}$	6	No	8.11	No
80	69	7	2	9	1	8	Maybe	8.11	Yes
80	70	6	2	9	$\alpha^8$	8	Maybe	8.11	Yes
48	37	7	2	7	$\alpha^{20}$	9	Maybe	8.13	Yes
48	38	6	2	7	$\alpha$	8	Maybe	8.13	Yes
48	39	5	2	7	2	8	No	8.13	No
48	39	4	2	7	3	8	No	8.13	No
48	39	5	2	7	$\alpha^6$	8	No	8.13	No

**Theorem 8.5.** Let  $(p, q) = (2, 4)$  and  $m \geq 3$ . Then the code  $C_s$  defined by the sequence of Lemma 8.4 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$



and  $\mathbb{L}_s$  are given in Lemma 8.4, and

$$\begin{cases} d = 2 & \text{if } a = 0 \text{ and } \delta(1) = 0 \text{ and } \gcd(5, n) = 5, \\ d = 3 & \text{if } a = 0 \text{ and } \delta(1) = 0 \text{ and } \gcd(5, n) = 1, \\ d = 4 & \text{if } a = 0 \text{ and } \delta(1) = 1, \\ d \geq 3 & \text{if } a = 1 \text{ and } \delta(1) = 0, \\ d \geq 4 & \text{if } a = 1 \text{ and } \delta(1) = 1, \\ d \geq 6 & \text{if } a + a^2 \neq 0 \text{ and } \delta(1) = 0, \\ d \geq 7 & \text{if } a + a^2 \neq 0 \text{ and } \delta(1) = 1. \end{cases}$$

*Proof.* The dimension of  $C_s$  follows from Lemma 8.4 and the definition of the code  $C_s$ . We need to prove the conclusion on the minimum distance  $d$  of  $C_s$ .

The proof of the lower bounds for the case  $a = 0$  is the same as that of Theorem 8.3. When  $a = 1$ ,  $\mathbb{M}_s(x)$  has the zeros  $\alpha^2$  and  $\alpha^3$ . Hence  $d \geq 3$  when  $a = 1$ . If  $\delta(1) = 1$ ,  $C_s$  is an even-weight code. Hence  $d \geq 4$  when  $a = 1$  and  $m$  is odd.

We finally consider the case that  $a + a^2 \neq 0$ . Note that  $\tilde{\mathbb{M}}_s(x)$  has the zeros  $\alpha^i$  for all  $i \in \{1, 2, 3, 4, 5\}$ , and the additional zero  $\alpha^0$  when  $\delta(1) = 1$ . The conclusions on the minimum weight  $d$  in this case follow from the BCH bound.  $\square$

Examples of the code of Theorem 8.5 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

We now consider the case  $(p, q) = (2, 2^t)$ , where  $t \geq 3$ , and prove the following lemma.

**Lemma 8.6.** *Let  $(p, q) = (2, 2^t)$  and  $m \geq 3$ , where  $t \geq 3$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-1}}(x) & \text{if } a = 0, \\ \prod_{i=2}^5 m_{\alpha^{-i}}(x) & \text{if } 1 + a + a^2 = 0, \\ (x-1)^{\delta(1+a+a^2)} \prod_{i=1}^5 m_{\alpha^{-i}}(x) & \text{if } a + a^2 + a^3 \neq 0, \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + 3m & \text{if } a = 0, \\ \delta(1) + 4m & \text{if } 1 + a + a^2 = 0, \\ \delta(1) + 5m & \text{if } a + a^2 + a^3 \neq 0. \end{cases}$$

*Proof.* Note that

$$D_5(x+1, a) = x^5 + x^4 + ax^3 + ax^2 + (1+a+a^2)x + 1 + a + a^2.$$

Since  $q = 2^t$ , where  $t \geq 3$ , we have then

$$\begin{aligned} \text{Tr}(D_5(x+1, a)) &= \text{Tr}(x^5 + x^4 + ax^3 + ax^2 + (1+a+a^2)x) \\ &\quad + \text{Tr}(1 + a + a^2). \end{aligned}$$

By definition,

$$\begin{aligned} s_t &= \text{Tr}((\alpha^t)^5 + (\alpha^t)^4 + a(\alpha^t)^3 + a(\alpha^t)^2 + (a+a^2)\alpha^t) + \\ (22) \quad &\text{Tr}(1 + a + a^2). \end{aligned}$$

It can be easily proved that  $\ell_i = m$  for all  $1 \leq i \leq 5$  and that these  $C_i$ , where  $1 \leq i \leq 5$ , are pairwise disjoint. The desired conclusions on the linear span and the minimal polynomial  $\mathbb{M}_s(x)$  then follow from Lemma 2.2 and (22).  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 8.7.** *Let  $(p, q) = (2, 2^t)$ , where  $t \geq 3$ . Then the code  $C_s$  defined by the sequence of Lemma 8.6 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 8.6, and*

$$\begin{cases} d \geq 3 & \text{if } a = 0 \text{ and } \delta(1) = 0, \\ d \geq 4 & \text{if } a = 0 \text{ and } \delta(1) = 1, \\ d \geq 5 & \text{if } 1 + a + a^2 = 0, \\ d \geq 6 & \text{if } a + a^2 + a^3 \neq 0 \text{ and } \delta(1) = 0, \\ d \geq 7 & \text{if } a + a^2 + a^3 \neq 0 \text{ and } \delta(1) = 1. \end{cases}$$

*Proof.* The proof of this theorem is similar to that of Theorem 8.5, and is omitted.  $\square$

Examples of the code of Theorem 8.7 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

We now consider the case  $q = p = 3$  and state the following lemma and theorem without proofs.

**Lemma 8.8.** *Let  $q = p = 3$  and  $m \geq 3$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1+a+2a^2)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x) & \text{if } a - a^6 = 0, \\ (x-1)^{\delta(1+a+2a^2)} \prod_{i=2}^5 m_{\alpha^{-i}}(x) & \text{if } a - a^6 \neq 0, \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1+a+2a^2) + 3m & \text{if } a - a^6 = 0, \\ \delta(1+a+2a^2) + 4m & \text{if } a - a^6 \neq 0. \end{cases}$$

*Proof.* The proof is similar to that of Lemma 8.6, and is omitted here.  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 8.9.** *Let  $q = p = 3$  and  $m \geq 3$ . Then the code  $C_s$  defined by the sequence of Lemma 8.8 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 8.8, and*

$$\begin{cases} d \geq 4 & \text{if } a - a^6 = 0, \\ d \geq 7 & \text{if } a - a^6 \neq 0 \text{ and } \delta(1+a+2a^2) = 0, \\ d \geq 8 & \text{if } a - a^6 \neq 0 \text{ and } \delta(1+a+2a^2) = 1. \end{cases}$$

*Proof.* The proof of this theorem is similar to that of Theorem 8.5, and is omitted.  $\square$

Examples of the code of Theorem 8.9 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

We now consider the case  $(p, q) = (3, 3^t)$ , where  $t \geq 3$ , and state the following lemma and theorem without proofs.

**Lemma 8.10.** *Let  $(p, q) = (3, 3^t)$  and  $m \geq 2$ , where  $t \geq 2$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is*

given by

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-1}}(x) & \text{if } 1+a=0, \\ (x-1)^{\delta(a-1)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) & \text{if } 1+a^2=0, \\ (x-1)^{\delta(1+a+2a^2)} \prod_{i=1}^5 m_{\alpha^{-i}}(x) & \text{if } (a+1)(a^2+1) \neq 0, \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1) + 4m & \text{if } a+1=0, \\ \delta(a-1) + 4m & \text{if } a^2+1=0, \\ \delta(1+a+2a^2) + 5m & \text{if } (a+1)(a^2+1) \neq 0. \end{cases}$$

*Proof.* The proof is similar to that of Lemma 8.6, and is omitted here.  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 8.11.** *Let  $(p, q) = (3, 3^t)$  and  $m \geq 2$ , where  $t \geq 2$ . Then the code  $C_s$  defined by the sequence of Lemma 8.6 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 8.10, and*

$$\begin{cases} d \geq 3 & \text{if } a = -1 \text{ and } \delta(1) = 0, \\ d \geq 4 & \text{if } a = -1 \text{ and } \delta(1) = 1, \\ d \geq 5 & \text{if } a^2 = -1 \text{ and } \delta(a-1) = 0, \\ d \geq 6 & \text{if } a^2 = -1 \text{ and } \delta(a-1) = 1, \\ d \geq 6 & \text{if } (a+1)(a^2+1) \neq 0 \text{ and } \delta(1+a+2a^2) = 0, \\ d \geq 7 & \text{if } (a+1)(a^2+1) \neq 0 \text{ and } \delta(1+a+2a^2) = 1. \end{cases}$$

*Proof.* The proof of this theorem is similar to that of Theorem 8.5, and is omitted.  $\square$

Examples of the code of Theorem 8.11 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

We finally consider the case  $p \geq 7$ , and present the following lemma and theorem without proofs.

**Lemma 8.12.** *Let  $p \geq 7$ . Let  $s^\infty$  be the sequence of (8), where  $f(x) = D_5(x, a) = x^5 - 5ax^3 + 5a^2x$ . Then the minimal polynomial  $\mathbb{M}_s(x)$  of  $s^\infty$  is given by*

$$\mathbb{M}_s(x) = \begin{cases} (x-1)^{\delta(1-5a+5a^2)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-1}}(x) & \text{if } a=2, \\ (x-1)^{\delta(1-5a+5a^2)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-1}}(x) & \text{if } a=\frac{2}{3}, \\ (x-1)^{\delta(1-5a+5a^2)} m_{\alpha^{-5}}(x) m_{\alpha^{-4}}(x) m_{\alpha^{-3}}(x) m_{\alpha^{-2}}(x) & \text{if } a^2-3a+1=0, \\ (x-1)^{\delta(1-5a+5a^2)} \prod_{i=1}^5 m_{\alpha^{-i}}(x) & \text{if } (a^2-3a+1)(a-2)(3a-2) \neq 0, \end{cases}$$

where  $m_{\alpha^{-j}}(x)$  and the function  $\delta(x)$  were defined in Section 2.1, and the linear span  $\mathbb{L}_s$  of  $s^\infty$  is given by

$$\mathbb{L}_s = \begin{cases} \delta(1-5a+5a^2) + 4m & \text{if } (a^2-3a+1)(a-2)(3a-2)=0, \\ \delta(1-5a+5a^2) + 5m & \text{otherwise.} \end{cases}$$

*Proof.* The proof is similar to that of Lemma 8.6, and is omitted here.  $\square$

The following theorem provides information on the code  $C_s$ .

**Theorem 8.13.** *Let  $p \geq 7$ . Then the code  $C_s$  defined by the sequence of Lemma 8.12 has parameters  $[n, n - \mathbb{L}_s, d]$  and generator polynomial  $\mathbb{M}_s(x)$ , where  $\mathbb{M}_s(x)$  and  $\mathbb{L}_s$  are given in Lemma 8.12, and*

$$\left\{ \begin{array}{ll} d \geq 3 & \text{if } a = 2 \text{ and } \delta(1 - 5a + 5a^2) = 0, \\ d \geq 4 & \text{if } a = 2 \text{ and } \delta(1 - 5a + 5a^2) = 1, \\ d \geq 4 & \text{if } a = \frac{2}{3} \text{ and } \delta(1 - 5a + 5a^2) = 0, \\ d \geq 5 & \text{if } a = \frac{2}{3} \text{ and } \delta(1 - 5a + 5a^2) = 1, \\ d \geq 5 & \text{if } 1 - 3a + a^2 = 0 \text{ and } \delta(1 - 5a + 5a^2) = 0, \\ d \geq 6 & \text{if } 1 - 3a + a^2 = 0 \text{ and } \delta(1 - 5a + 5a^2) = 1, \\ d \geq 6 & \text{if } (a^2 - 3a + 1)(a - 2)(3a - 2) \neq 0 \text{ and} \\ & \delta(1 - 5a + 5a^2) = 0, \\ d \geq 7 & \text{if } (a^2 - 3a + 1)(a - 2)(3a - 2) \neq 0 \text{ and} \\ & \delta(1 - 5a + 5a^2) = 1. \end{array} \right.$$

*Proof.* The proof of this theorem is similar to that of Theorem 8.5, and is omitted.  $\square$

Examples of the code of Theorem 8.13 are summarized in Table 5, where the meanings of the entries are the same as those in Table 1.

#### 9. CYCLIC CODES FROM OTHER $D_i(x, a)$ FOR $i \geq 6$

Parameters of cyclic codes from  $D_i(x, a)$  for  $i \geq 6$  may be established in a similar way. However, more cases are involved and the situation is getting more complicated when  $i$  gets bigger. In this section, employing  $D_7(x, a)$  and  $D_{11}(x, a)$  we will compute only some examples of optimal cyclic codes or cyclic codes having the same parameters as the best linear codes known in the Database that were not obtained by Dickson polynomials of smaller degrees before. These examples of cyclic codes are summarized in Table 6 and should be used to update the Database, where the meanings of the entries are the same as those in Table 1.

#### 10. CYCLIC CODES FROM DICKSON POLYNOMIALS OF THE SECOND KIND

Theorems on cyclic codes from Dickson polynomials of the second kind can be developed in a similar way as what we did for those from Dickson polynomials of the first kind in previous sections. We leave this to the interested reader. Instead, we will compute and report only examples of cyclic codes from Dickson polynomials of the second kind that can be used to update the Database of record linear codes. We are interested in only cyclic codes with parameters that cannot be obtained from cyclic codes defined by Dickson polynomials of the first kind. Examples of these cyclic codes are summarized in Table 7, where the meanings of the entries are the same as those in Table 1.

#### 11. MORE CYCLIC CODES FROM DICKSON POLYNOMIALS

The construction of sequences and their cyclic codes of Section 3 is generic. In (8), we may choose

$$f(x) = D_h(x, a) - 1$$

or

$$f(x) = E_h(x, a) - 1.$$

TABLE 6. Cyclic codes from  $D_i(x, a)$ ,  $i \in \{7, 11\}$ 

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	$D_i(x, a)$	DB
30	10	12	5	2	$\alpha$	12	Yes	$D_{11}(x, a)$	Yes
30	11	11	5	2	$\alpha^3$	11	Yes	$D_{11}(x, a)$	Yes
80	59	9	4	3	$\alpha$	12	Maybe	$D_7(x, a)$	Yes
80	60	8	4	3	$\alpha^2$	12	Maybe	$D_7(x, a)$	Yes
15	3	11	2	4	$\alpha$	11	Yes	$D_7(x, a)$	Yes
15	4	10	2	4	$\alpha^7$	10	Yes	$D_7(x, a)$	Yes
15	5	8	2	4	$\alpha$	8	Yes	$D_{11}(x, a)$	Yes
15	13	2	2	4	1	2	Yes	$D_{11}(x, a)$	Yes
63	45	9	3	4	$\alpha^5$	13	Maybe	$D_7(x, a)$	Yes
63	44	10	3	4	$\alpha$	14	Maybe	$D_7(x, a)$	Yes
63	47	8	3	4	0	11	Maybe	$D_{11}(x, a)$	Yes
24	8	13	2	5	$\alpha^{17}$	13	Yes	$D_{11}(x, a)$	Yes
24	9	12	2	5	$\alpha^{20}$	13	Maybe	$D_{11}(x, a)$	Yes
124	96	13	3	5	1	20	Maybe	$D_{11}(x, a)$	Yes
63	48	10	2	8	$\alpha$	13	Maybe	$D_7(x, a)$	Yes
63	49	9	2	8	$\alpha^{23}$	12	Maybe	$D_7(x, a)$	Yes
80	65	9	2	9	$\alpha$	13	Maybe	$D_7(x, a)$	Yes
80	66	8	2	9	$\alpha^{23}$	12	Yes	$D_7(x, a)$	Yes

TABLE 7. Examples of cyclic codes from  $E_i(x, a)$ 

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	$E_i(x, a)$	DB
8	6	2	2	3	$\alpha$	2	Yes	$E_3(x, a)$	Yes
26	22	3	3	3	$\alpha^8$	3	Yes	$E_3(x, a)$	Yes
80	76	2	4	3	$\alpha^{21}$	2	Yes	$E_3(x, a)$	Yes
242	237	2	5	3	$\alpha^{37}$	2	Yes	$E_3(x, a)$	Yes
242	236	3	5	3	$\alpha$	3	Yes	$E_3(x, a)$	Yes
15	10	4	4	2	$\alpha$	4	Yes	$E_5(x, a)$	Yes

In this way, the new code is the same as the code defined by  $D_h(x, a)$  or  $E_h(x, a)$  or its dimension is one more or less than the dimension of the code defined by  $D_h(x, a)$  or  $E_h(x, a)$ . So new codes may be obtained. In this section, we present a number of new codes obtained in this way. Again, in Table 8 we will list optimal cyclic codes or those that should be used to employ the Database and were not obtained in previous sections.

## 12. CONCLUDING REMARKS

In this paper, we studied the codes derived from Dickson polynomials of the first and second kind with small degrees. It is amazing that in most cases the cyclic codes derived from Dickson polynomials within the framework of this paper are optimal or almost optimal. About 90 linear codes in the Database should be replaced with these cyclic codes presented in this paper, as these cyclic codes are either optimal or have the same parameters

TABLE 8. More cyclic codes from  $D_i(x, a)$ 

$n$	$k$	$d$	$m$	$q$	$a$	Bd.	Opt.	$D_i(x, a)$	DB
48	43	4	2	7	$\alpha^{37}$	4	Yes	$D_2(x, a)$	Yes
80	75	4	2	9	$\alpha^9$	4	Yes	$D_2(x, a)$	Yes
7	4	3	2	2	1	3	Yes	$D_5(x, a)$	Yes
127	106	7	7	2	1	8	Maybe	$D_5(x, a)$	Yes
242	221	8	5	3	2	10	Maybe	$D_5(x, a)$	Yes
242	222	7	5	3	$\alpha^{122}$	9	Maybe	$D_5(x, a)$	Yes
242	227	5	5	3	1	6	Maybe	$D_5(x, a)$	Yes
24	22	2	2	5	$\alpha^{13}$	2	Yes	$D_5(x, a)$	Yes
124	121	2	3	2	3	2	Yes	$D_5(x, a)$	Yes

as the record linear codes in the database and have efficient encoding and decoding algorithms. A full version of this paper will be posted on arxiv, which contains the generator polynomials of the cyclic codes presented in this paper.

It is known that on average the error correcting capability of cyclic codes is not as good as that of linear codes. However, it was demonstrated in this paper that many cyclic codes are in fact optimal linear codes. The cyclic codes presented in this paper were obtained with simple arithmetic in finite fields and have a simple algebraic description.

We had to treat Dickson polynomials of small degrees case by case over finite fields with different characteristics as we did not see any way to treat them in a single strike. The generator polynomial and the dimension of the codes depend heavily on the degree of the Dickson polynomials and the characteristic of the base field.

Experimental data indicates that the codes from the Dickson polynomials of the first kind are in general better than those from the Dickson polynomials of the second kind, though some cyclic codes from Dickson polynomials of the second kind could also be optimal or almost optimal.

It should be noted that not all cyclic codes presented in this paper are new. Some of them are equivalent to some known family of cyclic codes in the literature. However, it is interesting to show that they can be produced when Dickson polynomials of very small degrees are plugged into the construction approach of this paper.

The idea of constructing cyclic codes employed in this paper looks simple, but was proven to be very promising in this paper. It would be nice if other polynomials of special forms over finite fields can be employed in this approach to produce more optimal and almost optimal cyclic codes.

## REFERENCES

- [1] M. Antweiler, L. Bomer, "Complex sequences over  $\text{GF}(p^M)$  with a two-level autocorrelation function and a large linear span," *IEEE Trans. Inform. Theory*, vol. 38, pp. 120–130, 1992.
- [2] C. Carlet, C. Ding, J. Yuan, "Linear codes from highly nonlinear functions and their secret sharing schemes," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 2089–2102, 2005.
- [3] P. Charpin, Open problems on cyclic codes, in: *Handbook of Coding Theory, Part 1: Algebraic Coding*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 11.
- [4] R. T. Chien, "Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Inform. Theory*, vol. 10, pp. 357–363, 1964.
- [5] R. S. Coulter, R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes Cryptogr.*, vol. 10, pp. 167–184, 1997.

TABLE 9. The minimal polynomial  $m_{\alpha}^{(q,m)}(x)$  of the generator  $\alpha$  of  $\text{GF}(r)^*$ 

$q$	$m$	primitive polynomial $m_{\alpha}^{(q,m)}(x)$
2	3	$x^3 + x + 1 \in \text{GF}(2)[x]$
2	4	$x^4 + x + 1 \in \text{GF}(2)[x]$
2	5	$x^5 + x^2 + 1 \in \text{GF}(2)[x]$
2	6	$x^6 + x^4 + x^3 + x + 1 \in \text{GF}(2)[x]$
2	7	$x^7 + x + 1 \in \text{GF}(2)[x]$
2	8	$x^8 + x^4 + x^3 + x^2 + 1 \in \text{GF}(2)[x]$
3	2	$x^2 + 2x + 2 \in \text{GF}(2)[x]$
3	3	$x^3 + 2x + 1 \in \text{GF}(2)[x]$
3	4	$x^4 + 2x^3 + 2 \in \text{GF}(2)[x]$
4	2	$x^4 + x + 1 \in \text{GF}(2)[x]$
4	3	$x^6 + x^4 + x^3 + x + 1 \in \text{GF}(2)[x]$
4	4	$x^8 + x^4 + x^3 + x^2 + 1 \in \text{GF}(2)[x]$
5	2	$x^2 + 4x + 2 \in \text{GF}(5)[x]$
5	3	$x^3 + 3x + 3 \in \text{GF}(5)[x]$
7	2	$x^2 + 6x + 3 \in \text{GF}(7)[x]$
8	2	$x^4 + 2x^3 + 2 \in \text{GF}(3)[x]$
9	2	$x^6 + x^4 + x^3 + x + 1 \in \text{GF}(2)[x]$

- [6] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group," *Ann. of Math.*, vol. 11, pp. 65–120, pp. 161–183, 1896/97.
- [7] C. Ding, "Cyclic codes from APN and planar functions," Preprint, 2012.
- [8] C. Ding, J. Yuan, "A family of skew Hadamard difference sets," *J. of Combinatorial Theory, Series A*, vol. 113, pp. 1526–1535, 2006.
- [9] G. D. Forney, "On decoding BCH codes," *IEEE Trans. Inform. Theory*, vol. 11, no. 4, pp. 549–557, 1995.
- [10] C. R. P. Hartmann, K. K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, pp. 489–498, 1972.
- [11] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [12] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Longman, England, 1993.
- [13] L. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [14] J. H. van Lint, R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 23–40, 1986.
- [15] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Air Force Cambridge Research Center-TN-58-156, Cambridge, Mass., April 1958.
- [16] J. Yuan, C. Carlet, C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 712–717, Feb. 2006.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY, CLEAR WATER BAY, KOWLOON, HONG KONG.

E-mail address: cding@ust.hk